Exhibit 38

US-CERT
UNITED STATES COMPUTER EMERGENCY READINESS TEAM

Search US-CERT

Advanced Options...

US-CERT Current Activity

RSS ATOM

The US-CERT Current Activity web page is a regularly updated summary of the most frequent, high-impact types of security incidents currently being reported to the US-CERT.

Last reviewed: December 1, 2005 16:49:16 EST

new	Reports of IRS Phishing Emails
updated	Exploit for Vulnerability in Microsoft Internet Explorer window() object
	Vulnerability in Cisco PIX
	W32/Sober Revisited
	First 4 Internet XCP (Sony DRM) Vulnerabilities
	Vulnerability in Macromedia Flash Player
	Oracle Worm Proof-of-Concept Code
	Exploit for Snort Back Orifice Preprocessor Buffer Overflow Vulnerability
	Multiple Vulnerabilities in Skype
	Vulnerabilities in Oracle Products
	Vulnerability in Snort Back Orifice Preprocessor
	Hurricane Tragedies Spawn Phishing Sites
	Vulnerability in Cisco IOS Firewall Authentication Proxy

Additional Information

- Ports Associated with Known Vulnerabilities and Exploits
- Current Activity Archive

National Cyber Alert System

Technical Cyber Security Alerts
Cyber Security Alerts
Cyber Security Bulletins
Cyber Security Tips

- Report an incident
- Report a vulnerability

General Tips

- Apply vendor-supplied software patches in a timely manner
- Disable features/services that are not explicitly required
- Install anti-virus software and keep it up to date
- Use caution when opening email attachments and following URLs

---

Reports of IRS Phishing Emails

added November 30, 2005

US-CERT has received reports of a phishing email scam that attempts to convince the user that it is from the Internal Revenue Service (IRS) by using a spoofed "From" address of "tax-refunds@irs.gov".

Upon clicking on the link provided in the email, the user is taken to a fraudulent site that looks like a legitimate U.S. government site. The user is then asked to provide personal information, such as their social security, credit card and bank pin numbers.

Users are encouraged to take the following measures to protect themselves from this type of phishing attack:

1. Do not follow unsolicited web links received in email messages.
2. Contact your financial institution immediately if you believe your account/and or financial information has been compromised.

For additional information on ways to avoid phishing email attacks, US-CERT recommends that all users reference the following:

- Avoiding Social Engineering and Phishing Attacks
- Spoofed/Forged Email

Exploit for Vulnerability in Microsoft Internet Explorer window() object

added November 21, 2005 | updated November 30, 2005

US-CERT is aware of a vulnerability in the way Microsoft Internet Explorer handles requests to the window() object. If exploited, the vulnerability could allow a remote attacker to execute arbitrary code with the privileges of the user. Additionally, the attacker could also cause IE (or the program using the WebBrowser control) to crash.

According to Microsoft, malicious software is targeting this vulnerability. We have confirmed that the proof-of-concept code is successful on Windows 2000 and Windows XP systems that are fully patched as of November 30, 2005.

More information about this vulnerability can be found in the following US-CERT Vulnerability Note:

- VU#887861 - Microsoft Internet Explorer vulnerable to code execution via scripting "window()" object

Until a patch is available to address this vulnerability, US-CERT strongly encourages Windows users to disable Active Scripting.

Additionally, Microsoft has updated its Security Advisory about this issue and is continuing to investigate the problem.

Vulnerability in Cisco PIX

added November 23, 2005 | updated November 28, 2005

US-CERT is aware of a publicly-reported vulnerability in the way Cisco PIX firewalls process legitimate TCP connection attempts. A remote attacker may be able to send spoofed, malformed TCP packets with incorrect checksum values through affected PIX firewalls. As a result, legitimate network traffic to the destination may be blocked until the invalid PIX connection-attempt entry times out (around two minutes by default).

Public exploit code for this reported vulnerability may be useful for automating a sustained attack. More information about the reported vulnerability can be found in the following US-CERT Vulnerability Note:

- VU#853540 - Cisco PIX TCP checksum verification failure report

Until a patch or more information becomes available, US-CERT recommends that system administrators who may be affected consider reconfiguring certain connection timers on Cisco PIX systems. More workaround information is also available in the solution section of VU#853540.

W32/Sober Revisited

added November 22, 2005 | updated November 22, 2005

US-CERT is aware of several new variants of the W32/Sober virus that propagate via email. As with many viruses, these variants rely on social engineering to propagate. Specifically, the user must click on a link or open an attached file.

A recent variant sends messages that appear to be from the CIA or FBI, while a German version appears to be coming from the Bundeskriminalamt (BKA), the

German Federal police service. US-CERT encourages users to review the appropriate alert below:

- FBI ALERTS PUBLIC TO RECENT E-MAIL SCHEME
- BKA warnt vor gefälschten E-Mails mit BKA-Absender - Variante des Sober-Wurms

These new variants of the W32/Sober virus identified above share common characteristics listed below. Once infected, the malicious code may:

- Attempt to harvest email addresses from a configurable list of file extensions
- Utilize its own SMTP engine to send itself to the harvested email addresses

Although each variant has different functionality, the list below contains a subset of the common characteristics found in previous variants. Once a system is infected, the malicious code may:

- Modify the system registry to prevent Windows XP's built-in firewall from starting
- Attempt to harvest email addresses from a configurable list of file extensions
- Utilize its own SMTP engine to send itself to the harvested email addresses
- Modify the HOSTS file to prevent the computer from accessing certain security and commercial web sites
- Attempt to terminate a number of running processes, some of which are security related
- Open a backdoor on the system that allows the attacker to communicate remotely with the system via IRC. This may allow the attacker to upload and execute arbitrary code on the infected machine.

US-CERT strongly encourages users to install anti-virus software, and keep its virus signature files up-to-date.

Additionally, US-CERT strongly encourages users not to follow unknown links, even if sent by a known and trusted source. You may also wish to visit the US-CERT Computer Virus Resources.

First 4 Internet XCP (Sony DRM) Vulnerabilities

added November 15, 2005 | updated November 18, 2005

US-CERT is aware of several vulnerabilities regarding the XCP Digital Rights Management (DRM) software by First 4 Internet, which is distributed by some Sony BMG audio CDs. The XCP copy protection software uses "rootkit" technology to hide certain files from the user. This technique can pose a security threat, as malware can take advantage of the ability to hide files. We are aware of malware that is currently using this technique to hide.

One of the uninstallation options provided by Sony also introduces vulnerabilities to a system. Upon submitting a request to uninstall the DRM software, the user will receive via email a link to a Sony BMG web page. This page will attempt to install an ActiveX control when it is displayed in Internet Explorer. This ActiveX control is marked "Safe for scripting," which means that any web page can utilize the control and its methods. Some of the methods provided by this control are dangerous, as they may allow an attacker to download and execute arbitrary code.

More information about this vulnerability can be found in the following US-CERT Vulnerability Note:

- VU#312073 - First 4 Internet XCP "Software Updater Control" ActiveX control incorrectly marked "safe for scripting"

US-CERT recommends the following ways to help prevent the installation of this type of rootkit:

- Do not run your system with administrative privileges. Without administrative privileges, the XCP DRM software will not install.
- Use caution when installing software. Do not install software from sources that you do not expect to contain software, such as an audio CD.
- Read the EULA (End User License Agreement) if you do decide to install software. This document can contain information about what the software may do.
- Disable automatically running CD-ROMs by editing the registry to change the Autorun value to 0 (zero) as described in Microsoft Article 155217.

Vulnerability in Macromedia Flash Player

added November 14, 2005 | updated November 17, 2005

US-CERT is aware of a buffer overflow vulnerability in Macromedia Flash Player versions 7.0.53.0 and earlier. If exploited, the vulnerability could allow a remote attacker to execute arbitrary code with privileges of the user on the affected system. We are not aware of any public exploits at this time.

More information about this vulnerability can be found in the following US-CERT Vulnerability Note:

- VU#146284 - Macromedia Flash Player fails to properly validate the frame type identifier read from a "SWF" file

US-CERT encourages users to upgrade to the appropriate software version as described in the Macromedia Security Bulletin MPSB05-07.

Oracle Worm Proof-of-Concept Code

added November 1, 2005 | updated November 7, 2005

US-CERT is aware of publicly available proof-of-concept code for an Oracle worm. Currently, US-CERT cannot confirm if this code works. We are working with Oracle to determine the threat posed by this code.

Although there is limited information concerning this potential threat, US-CERT strongly encourages Oracle system administrators to implement the following workarounds:

- Change default user credentials for Oracle installations
- Change the default port for the TNS listener
- Restrict Oracle network access to trusted hosts only
- Revoke CREATE DATABASE LINK privileges from the CONNECT role

For additional information on Oracle Database Security, please refer to the following webpage:

- http://www.oracle.com/technology/deploy/security/db_security/index.html

US-CERT will continue to investigate the issue and provide updates as they become available.

Exploit for Snort Back Orifice Preprocessor Buffer Overflow Vulnerability

added October 27, 2005

US-CERT is aware of publicly available exploit code for a buffer overflow vulnerability in the Snort Back Orifice preprocessor. This vulnerability may allow a remote, unauthenticated attacker to execute arbitrary code, possibly with root or SYSTEM privileges.

More information about this vulnerability can be found in the following:

- US-CERT Vulnerability Note: VU#175500 - Buffer overflow in Snort Back Orifice preprocessor
- Technical Cyber Security Alert: TA05-291A - Snort Back Orifice Preprocessor Buffer Overflow

US-CERT encourages Snort users to upgrade to version 2.4.3 as soon as possible. Until a fixed version of Snort can be deployed, disabling the Back Orifice preprocessor will mitigate this vulnerability.

Multiple Vulnerabilities in Skype

added October 26, 2005

US-CERT is aware of several buffer overflow vulnerabilities in Skype that may allow a remote attacker to execute arbitrary code.

The most critical of these issues can be exploited by sending a specially crafted packet to a vulnerable Skype installation. More information about this vulnerability can be found in the following US-CERT Vulnerability Note:

- VU#905177 - Skype vulnerable to heap-based buffer overflow

The other two vulnerabilities can be exploited by accessing a specially crafted VCARD or Skype URI. More information about these vulnerabilities can be found in the following US-CERT Vulnerability Notes:

- VU#668193 - Skype VCARD handling routine contains a buffer overflow
- VU#930345 - Skype URI handling routine contains a buffer overflow

Skype has released the following Security Bulletins to address these vulnerabilities:

- SKYPE-SB/2005-003 to address VU#905177
- SKYPE-SB/2005-002 to address VU#668193 and VU#930345

US-CERT encourages Skype users to upgrade to the latest fixed version of Skype as soon as possible.

Vulnerabilities in Oracle Products

added October 19, 2005

US-CERT is aware of multiple vulnerabilities in Oracle products. The impact of these vulnerabilities varies depending on the product, component, and configuration of the system. Potential consequences include remote execution of arbitrary code or commands, access to sensitive information, and denial of service.

Many of these vulnerabilities are corrected by the Oracle Critical Patch Update (CPU) for October 2005. According to public reports, the patches included in this update, as well as previous updates, may not adequately correct all security vulnerabilities.

More information about this vulnerability can be found in the following:

- US-CERT Vulnerability Note: VU#210524 - Oracle products contain multiple vulnerabilities
- Technical Cyber Security Alert: TA05-292A - Oracle products contain multiple vulnerabilities
- Oracle Critical Patch Update - October 2005

US-CERT is continuing to investigate these reports and will provide further information as it becomes available.

Vulnerability in Snort Back Orifice Preprocessor

added October 18, 2005

US-CERT is aware of a buffer overflow vulnerability in the Snort Back Orifice preprocessor. If exploited, the vulnerability could allow a remote, unauthenticated attacker to execute arbitrary code with possibly root or SYSTEM privileges on the affected system. We are not aware of any public exploits at this time.

More information about this vulnerability can be found in the following:

- US-CERT Vulnerability Note: VU#175500 - Buffer overflow in Snort Back Orifice preprocessor
- Technical Cyber Security Alert: TA05-291A - Snort Back Orifice Preprocessor Buffer Overflow

US-CERT encourages Snort users to upgrade to version 2.4.3 as soon as possible.

Hurricane Tragedies Spawn Phishing Sites

added August 31, 2005 | updated September 23, 2005

US-CERT warns users to expect an increase in targeted phishing emails due to recent events such as Hurricane Katrina and Hurricane Rita. US-CERT has received reports of multiple phishing sites that attempt to trick users into

donating funds to fraudulent foundations in the aftermath of Hurricane Katrina. US-CERT expects to see the same type of malicious activity during the aftermath of Hurricane Rita.

Phishing emails may appear as requests from a charitable organization asking the users to click on a link that will then take them to a fraudulent site that appears to be a legitimate charity. The users are then asked to provide personal information that can further expose them to future compromises.

Users are encouraged to take the following measures to protect themselves from this type of phishing attack:

1. Do not follow unsolicited web links received in email messages
2. Contact your financial institution immediately if you believe your account/and or financial information has been compromised

US-CERT strongly recommends that all users reference the Federal Emergency Management Agency (FEMA)web site for a list of legitimate charities to donate to their charity of choice.

Vulnerability in Cisco IOS Firewall Authentication Proxy

added September 8, 2005

US-CERT is aware of a buffer overflow vulnerability in Cisco IOS Firewall Authentication Proxy for FTP and Telnet Sessions. If exploited, the vulnerability could allow a remote unauthenticated attacker to execute arbitrary code or cause a denial-of-service condition on the affected system. We are not aware of any public exploits at this time.

More information about this vulnerability can be found in the following US-CERT Vulnerability Note:

- VU#236045 - Cisco IOS Firewall Authentication Proxy vulnerable to buffer overflow via specially crafted user authentication credentials

US-CERT urges users to review the fixes, updates, and workarounds described in the Cisco Security Advisory.
